② Дедекиндовы кольца

1. Опр-е и св-ва элем. св-ва

Опр. Кольцо A наз-ся **дедекиндовым**, если оно

1) обл. целостности
2) нётерово
3) целозамкнуто
4) любой ненулевой простой идеал максимален

Напоминание: $I \trianglelefteq A$ простой $\Leftrightarrow$ A/I обл. целост.

$I \trianglelefteq A$ макс. $\Leftrightarrow$ A/I — поле, т.е.

макс $\Rightarrow$ простой всегда

4) простой $\Rightarrow$ макс в дедекинд. кольцах.

<u>Предл 1</u> Обл. главных идеалов — дедекиндово кольцо.

<u>Д-во:</u> Пп. 1) и 2) Опр 1, очевидно, выполнены.

3) следует из факториальности Обл. гл. идеалов (см. Упр 4 в ANT0-решении на семинаре), т.к. факториальность $\Rightarrow$ целозамкнутость (Т. 1.1.2 из ANT 1)

4) Пусть $I \underset{\text{простой}}{\trianglelefteq} A$. Т.к. A Обл. гл. идеалов $\Rightarrow I = (p)$, где p — простой. Если $x \notin I$, то $(x, p) = 1 \Rightarrow$
$\exists\, a, b : ax + bp = 1 \Rightarrow ax \in 1 + I \Rightarrow (x+I)^{-1} = a + I$
$\Rightarrow A/I$ — поле $\Rightarrow I$ макс. ■

<u>Упр 1</u> Пусть F — поле. При каких n $F[x_1 \ldots x_n]$ — дедекиндово?

Предл 2 Если A — дедекиндово и факториальное, то в A любой ненул. простой идеал — главный.

Д-во: Пусть $0 \neq I \underset{\text{простой}}{\trianglelefteq} A$. Кольцо A факториально

$\underset{\neq 0}{\forall x} \in I \quad \exists$ неприв. $p_1, \dots, p_n$: $x = p_1 \cdots p_n$, причем

$n \geq 1$, т.к. x необратим (иначе $I = A$)

Т.к. I - простой, то в A/I нет делителей нуля

$\Rightarrow \exists\, i \in \{1, \dots, n\}$: $p = p_i \in I \Rightarrow 0 \neq (p) \subseteq I \subseteq A$.

p - неприв. $\underset{\text{(факт.)}}{\Longrightarrow}$ p - простой $\underset{\text{(дедекин)}}{\Longrightarrow}$ $(p) \underset{\max}{\triangleleft} A \Rightarrow (p) = I$

Лемма Пусть обл. целостности $B \supseteq F$ - поле и B цел. над F.
Тогда B - поле.

Д-во: Достаточно $\forall z \neq 0 \in B$ найти обр. к нему. Р-м
от-е $\varphi : F[z] \to F[z]$ по правилу $\varphi(x) = xz$.
φ инъективно, т.к. B - обл. целостности. Более того,
φ сюръективно, т.к. $|F[z] : F| < \infty$ из-за того, что
z цел $\Rightarrow$ алгебраичен над F.
Поэтому φ - биекция $\Rightarrow \exists\, z^{-1} \in F[z] : z \cdot z^{-1} = 1$ ∎

Теорема Пусть A - дедекиндово кольцо, $K = Q(A)$ - поле частных,
$L \supset K$ - кон. сеп. расш. и $B = \overline{A}^{L}$ - целое замыкание A в L.
Тогда B - дедекиндово кольцо.

Д-во: 1) $B \subseteq L \Rightarrow B$ — обл. целостности

2) B нётерово, т.к. A нётерово (т. 1.4.1 о целом базисе)

3) B целозамк., т.к. A целозамкнуто (следствие 2 из предл. 1.2.2 о транзитивности целой зависимости)

Осталось проверить 4) $0 = q \underset{\text{прост}}{\trianglelefteq} B \Rightarrow q \underset{\max}{\trianglelefteq} B$, т.е. B/q — поле.

Рассмотрим $p = q \cap A \trianglelefteq A$.

а) $1 \notin q \Rightarrow 1 \notin p \Rightarrow p \neq A \Rightarrow p$ — собств. идеал в A.

б) $p \neq 0$, т.к. для $\underset{\neq 0}{z} \in q$ найдётся унитарный мн-н $h(t) = t^m + \ldots + a_1 t + a_0 \in A[t]$ наим. возм. степени m т.ч. $h(z) = 0$. Тогда $a_0 \neq 0$ (из min m) и $a_0 = -z^m - \ldots - a_1 z \in Az \subseteq q \Rightarrow$ $0 \neq a_0 \in p = q \cap A$.

в) $p \triangleleft_{\text{прост}} A$, т.к. $A/p = A/q\cap A \simeq (A+q)/q \subseteq B/q \Rightarrow$

A/p область целост.

A дедекиндово $\Rightarrow$ из пр-сти p следует максим. $\Rightarrow$ A/p – поле.

B цело над A $\Rightarrow$ B/q цело над A/p.

По лемме 1 B/q – поле $\Rightarrow$ $q \triangleleft_{\max} B$ ∎

<u>Следствие</u> L – алг. числовое поле $\Rightarrow$ O_L дедекиндово.

<u>Д-во:</u> Положить $A = \mathbb{Z}$.

Предл 3 Пусть S - мультипл. подмн-во дедекиндова кольца R. Тогда его локализация R_S дедекиндова.

Д-во: 1) R_S – обл. целостности, т.к $R_S = \{ \frac{f}{g} \mid g \in S\} \subseteq Q(R)$

3) R_S целозамк, в силу предл. 1.2.3 из ANT1 и целоз. R.

По т. 1.1.1 каждому простому идеалу pR_S в R_S соотв. простой идеал p в R, не пересекающий S, причем $pR_S \cap R = p$. Если бы сущ. $I \trianglelefteq R_S$: $pR_S \subset I \subset R_S$, то $p \subset I \cap R \underset{\neq}{\trianglelefteq} R$, противоречие $\Rightarrow$ 4) верно.

2) $I \trianglelefteq R_S \Rightarrow J = I \cap R \trianglelefteq R$. Т.к R нётерово, то $J = I \cap R = \langle a_1 .. a_n \rangle \Rightarrow I = J R_S$ (см. док-во т. 1.1.1) $=$

$= a_1 R + .. + a_n R$ – к.п. $\blacksquare$

Кит. теор. о „факториальности“ в дедекиндовых кольцах

Если $p \trianglelefteq_{\text{прост}} A$ дедекиндово $\Rightarrow pA_p \trianglelefteq_{\text{прост}} A_p$ — в локализации, где $A_p = A_{\{A \setminus \{p\}\}}$ $\Rightarrow I = pA_p$ — единств. простой идеал в A_p, т.к. в локальном кольце только один макс. идеал (простой = макс. из дедекин. A_p).

Опр 2 $I, J \trianglelefteq A$ взаимно просты, если $I + J = A$.

Аналогия в $\mathbb{Z}$: $(m, n) = 1 \Leftrightarrow (m) + (n) = \mathbb{Z}$

Лемма 2 I, J вз. пр. $\Rightarrow I^k, J^l$ вз. просты $\forall k, l \in \mathbb{N}$.

Д-во: Пусть $a \in I$, $b \in J$: $a + b = 1$. Для $n = k + l - 1$ имеем

$$1 = (a+b)^n = \left(a^n + C_n^1 a^{n-1} b + \ldots + C_n^k a^k b^{n-k}\right) + \left(C_n^{k-1} a^{k-1} b^l + \ldots + b^n\right) \in I^k + J^l$$

$\boxed{\text{Кв}}$

Предл. 4 Пусть $\mathfrak{p}$ – макс. идеал обл. целостности R и $\mathfrak{q} = \mathfrak{p}R_\mathfrak{p}$ – соотв. ему идеал в локализации $R_\mathfrak{p}$ кольца R.

Тогда $R/\mathfrak{p}^m \simeq R_\mathfrak{p}/\mathfrak{p}^m R_\mathfrak{p} \underset{\uparrow}{=} R_\mathfrak{p}/\mathfrak{q}^m \ \forall m \in \mathbb{N}$

Д-во: Имеем $\mathfrak{q}^m = (\mathfrak{p}R_\mathfrak{p})^m = \mathfrak{p}^m (R_\mathfrak{p})^m = \mathfrak{p}^m R$.

Р-м от-е $\varphi : R \to R_\mathfrak{p}/\mathfrak{p}^m R_\mathfrak{p}$, где $a \overset{\varphi}{\to} \frac{a}{1} + \mathfrak{p}^m R_\mathfrak{p}$.

Это от-е, очевидно, гом. зл. и $\operatorname{Ker}\varphi = \mathfrak{p}^m R_\mathfrak{p} \cap R = \mathfrak{p}^m$ (соотв-е идеалов). По т. о гом. мах осталось док-ть сюръективность φ.

$\forall \frac{b}{s} \in R_\mathfrak{p}$, $s \in S = R \setminus \mathfrak{p} \underset{\uparrow}{\Rightarrow} sR + \mathfrak{p} = R \underset{1.2}{\Rightarrow} sR + \mathfrak{p}^m = R$

макс. идеал $\mathfrak{p}$

Поэтому $\exists\, c \in R$ и $t \in p^n$: $cs + t = 1 \Rightarrow c = \frac{1-t}{s}$

Тогда $\varphi(bc) = \frac{bc}{1} + p^n R_p = \frac{b}{s} - \underset{p^n R_p}{\underset{\cap}{t\left(\frac{1}{s}\right)}} + p^n R_p =$

$= \frac{b}{s} + p^n R_p$, ч.т.д. ∎

<u>Упр 2</u>. Д-ть, что $\mathbb{Z}[1/p]$ — дедекиндово $\forall$ простого p.

<u>Теорема 2</u> Пусть A — нётерова целозамкн. обл. целостности, $0 \neq p \trianglelefteq A$ — единств. простой идеал. Тогда A — обл. главн. идеалов, причём любой $0 \neq I \trianglelefteq A$ имеет вид $I = p^n$ для $n \in \mathbb{N}$.

<u>Д-во:</u> 1) Докажем, что $p = xA$ — главный идеал.

Выберем $0 \neq a \in p$. Заметим, что $aA \subseteq p$.

Положим $\forall\, m \in A$ $I(a:m) = \{\ell \in A \mid \ell m \in aA\}$. Тогда

$I(a:m) \trianglelefteq A$, $a \in I(a:m)$ $\forall m \in A$ и $m \notin aA \Rightarrow I(a:m) \neq A$.

Выберем $b \notin aA$: $I(a:b)$ максимален среди всех $I(a:m)$, где $m \notin aA$. Сделать это можно в силу нётеровости A. Пусть $q = I(a:b)$.

Д-ем, что q - простой идеал. Если $u, v \in A$: $uv \in q$, то $uvb \in aA$. Если $u \notin q$ и $v \notin q$, то $ub \notin aA$ и $vb \notin aA$

Очевидно, $I(a:vb) \supseteq I(a:b)$. Т.к. $vb \notin A$ $\xRightarrow[\text{из макс. } I(a:b)]{}$

$I(a:vb) = I(a:b)$, но $u \in I(a:vb) \setminus I(a:b)$, против.

Т.к. p - единств. простой, имеем $q = I(a:b) = p$.

Сл-но, $pb \subseteq aA$. С др. стороны, $b \notin aA \Rightarrow \frac{b}{a} \in Q(A) \setminus A$.

Докажем, что $\frac{a}{b} \in A$ и $p = (\frac{a}{b})$ - главный.

Т.к. $pb \subseteq aA \Rightarrow p\frac{b}{a} \trianglelefteq A$.

Пред, что $p\frac{b}{a} \subseteq p$. Тогда p — $A[\frac{b}{a}]$-модуль,
к.п. над A (в силу нётеровости A) и точный, т.к. в
$A[\frac{b}{a}] \subseteq Q(A)$ нет делителей нуля, значит, в силу
предл. 1.2.1 о св-вах целой зависимости (из п.4 $\Rightarrow$ п.1)
имеем $\frac{b}{a}$ цел над A $\underset{\text{целозам. } A}{\Rightarrow}$ $\frac{b}{a} \in A$, противоречие.

Если $p\frac{b}{a} \subset A$, то в силу нётеровости A, $p\frac{b}{a} \subseteq I \trianglelefteq_{max} A$
Но макс. идеал I прост $\Rightarrow I = p$, противоречие.

Итак, $p\frac{b}{a} = A \Rightarrow p = \frac{a}{b}A \Rightarrow x = \frac{a}{b} \in A$ и $p = (x)$.

2) Пусть теперь $0 \neq I \trianglelefteq A$. Д-ем, что $I = (x^n)$ для некот. $n \in \mathbb{N}$,
где $p = (x) = xA$.

Т.к. $xI \subseteq I \Rightarrow I \subseteq x^{-1}I \subseteq Q(A)$. Имеем вложения

$(*)$ $I \subseteq x^{-1}I \subseteq x^{-2}I \subseteq \ldots$

Если $x^{-m}I = x^{(-m+1)}I$, то $x^{-m}I$ замк. отн-но умножения на x^{-1} $\Rightarrow x^{-m}$ – точный $A[x^{-1}]$-модуль

Кроме того, $x^{-m}I$ – к.п. над A, т.к. I – к.п. над A в силу нётеровости A. Снова применяя предл. 1.7.1, имеем x^{-1} цело над A $\underset{\text{целозам.}}{\Rightarrow}$ $x^{-1} = \frac{b}{a} \in A$, противоречие.

Поэтому все вложения в $(*)$ – строгие.

Найдем $n \in \mathbb{N}_0$: $x^{-n}I \subseteq A$ $(n \geq 0)$: $x^{-n-1}I \not\subseteq A$, такое и сущ. в силу нётеровости A. Заметим, что $x^{-n}I \not\subseteq p$, сначала $x^{-n}I \subseteq xA = p \Rightarrow x^{-n-1}I \subseteq A$, против.

Если $x^{-n} I \trianglelefteq A$ – собств., то он вкл. в макс $\Rightarrow$ выпадывается в p, что невозм. $\Rightarrow x^{-n} I = A \Rightarrow I = x^n A$ $\blacksquare$

<u>Следствие</u> Пусть A – дедекиндово, $0 \neq p \trianglelefteq A$, $m \in \mathbb{N}$.
Если $I \trianglelefteq A/p^m$, то $I = \left(p/p^m\right)^n = p^n/p^m$ для некоторого $1 \leq n \leq m$.

<u>1-во:</u> В силу предл 4 $A/p^m \simeq A_p/p^m A_p$, где $A_p = A_{\{A \setminus p\}}$ – локализация кольца A, соотв. идеалу p.
A_p – дедекиндово локальное кольцо $\Rightarrow pA_p$ – единств. простой идеал в A_p. По т. 2 любой идеал $J \trianglelefteq A_p$ имеет вид $J = p^n A_p$. Т.к. $A/p^m \simeq A_p/p^m A_p$, то образ I равен $p^n A_p / p^m A_p$, где $n \leq m$ ($n = m$ при $I = 0$) $\blacksquare$

<u>Упр 3</u> Записать аккуратно, почему $I \simeq p^n A_p / p^m A_p$.

<u>Указ:</u> См. д-во предл. 4 $\varphi: A/p^m \to A_p/p^m A_p$ так $x + p^m \mapsto \frac{x}{1} + p^m A_p$.